ACEEE *Proc. of Int. Conf.* on *Recent Trends in Information, Telecommunication and Computing, ITC*

Review of Heterogeneous/Homogeneous Wireless Sensor Networks and Intrusion Detection System Techniques

Prachi Uplap[1] and Preeti Sharma[2]
[1] Department of Computer Engineering,
SKN-Sinhagad Institute of Technology & Science, Lonavala, India
Email: prachiuplap22@gmail.com
[2] Department of Computer Engineering,
SKN-Sinhagad Institute of Technology & Science, Lonavala, India
Email: preeti5588@gmail.com

***Abstract*— Wireless sensor networks are made up of number of tiny mobile nodes, which have the capability of computation, sensing and wireless network communication. The energy efficiency of each node in such kind of networks is one of the important issues under consideration. Thus for these networks, sensor nodes life time is basically depends on use of routing protocols for routing operations in WSN. There are various routing protocols proposed by different researchers, which are considered as efficient on the basis of performance of network lifetime and energy scavenging. There are different routing protocols introduced for WSN such as flat routing protocols, clustering routing protocols, hierarchical routing protocols etc. On the other hand, there are basically two types of WSNs, homogeneous and heterogeneous sensor networks. As WSN is vulnerable to different types of security threats, there are many security methods presented with their own advantages and disadvantages. Most of security methods are applied only on homogeneous WSN, but recently some methods were presented to provide the routing security in heterogeneous WSNs as well. In this paper, the different security threats and Intrusions in WSNs are presented, with review of different security methods.**

***Index Terms*— Heterogeneous WSN, Homogeneous WSN, Security, IDS, Intrusions.**

I. INTRODUCTION

A wireless sensor network (WSN) is a network of economical and simple processing devices that are called as sensor nodes. For example, these sensors can be used as environmental sensors for sensing temperature. Sensors communicate with each other using a wireless radio device. In wireless sensor network most of applications require large number of sensor nodes. But this crowding of nodes generates problem while deploying the network. The wireless sensor network has been deployed with different wireless networking technologies. The 802.11 protocol is the first standard protocol for wireless local area networks (WLAN), which was introduced in 1997. After that it was upgraded to 802.11b with data rate increased and CSMA/CA mechanism for medium access control (MAC) [1, 2, 3].

The evolution of sensor node has a long history, from remote sensing to physical world observation for humans. This sensor technology is basically developed for defence applications. In defence, they used

DOI: 02.ITC.2014.5.574
© Association of Computer Electronics and Electrical Engineers, 2014

sensors for observing battlefield activities. In 1996 UCLA and Rockwell Science Centre developed Low Power Wireless Integrated Micro sensors (LWIM).It has ability to use low cost CMOS fabrication integrate multiple sensors, electronic interfaces, control, and communication on a single device. In 1998 this team developed second generation sensor node by applying some innovations which was named as Wireless Integrated Network Sensors (WINS) [2] [5] [6]. These WINS had a processor board with an Intel strong ARM SA1100 32-bit embedded processor (1 MB SRAM and 4 MB flash memory), radio board that supports 100 kbps with adjustable power consumption from 1 to 100 mW, a power supply board, and sensor board.

As we know, wireless mobile network is made up of mobile nodes which are capable of maintaining the wireless communication channel among them without depending on any kind of fixed infrastructure. Such factors are more enough to make them different from the wired networks like for the wireless networks there is no single access point, all the network nodes should be involved in the creation of network as well as infrastructure setups and services like routing and data collection. All the operations in MANET or WSN are conducted in a distributed manner as compared to the wired networks. So this is all about the wired and wireless networks differentiations. Nowadays this technology is used in many real world applications like organization, home appliances etc. In organizations, wireless sensor networks are used for intrusion detection for detecting attacks which are trying to get the information from the organization [6].

We can define the term intrusion as a set of actions, which are used for system alteration or unauthorized user access. Main task of the Intrusion Detection Systems (IDS), is to carry out the monitoring of systems and computer networks, detecting all the possible intrusions in those networks, user's alteration, etc. After the detection of intrusions network reconfiguration is done if possible. In literature we have studied many existing methods for the intrusion detection in WSN. Each method has its own advantages and disadvantages. In the real time applications, heterogeneous WSNs are frequently used for the important information sharing as compared to homogeneous WSNs. Hence there must have efficient multi sensing IDS system in place to provide the security to WSNs.

Recently some work has been done over the IDS through the routing protocol for heterogeneous WSNs. In this paper our aim is to present the review of IDS mechanism in WSN, review of literature and methods presented for IDS in WSN, introduction to homogeneous and heterogeneous WSNs and giving a comparative study among single sensing and multi sensing WSN. Finally we also give a possible future direction in the particular research field. In Section II, discussion over different methods presented for IDS in WSN is done. In section III introduction to homogeneous as well as heterogeneous WSNs with single sensing and multi sensing approaches are briefly described. In section IV, we are discussing the different IDS techniques and attacks in WSN. This paper is concluded with a glimpse of the proposed work where we have used intrusion detection system and heterogeneous wireless sensor network for detecting various attacks.

II. NEED OF IDS IN WSN

WSN means one type of network where multiple sensors scattered on the field for monitoring physical or environmental actions in the network. This network technology is basically developed for civil and military applications for defense network security. Nowadays this networks are used everywhere in organizations, home, offices etc. Intrusion detection system in wireless sensor network has become crucial for safe operation of wireless sensor network. The IDS is nothing but mechanism which is deployed into the sensor network protocols, which monitors malicious activities or policy violations and generates a report for management. There are several defense methods in WSNs but Intrusion detection system has become a major and efficient method against the intruders. In wireless sensor network to detect the attack in the network intrusion detection techniques is used. To implements the intrusion detection system in WSN, the sensor networks must have localized and partial audit information, because there are no centralized points in WSN for example routers, gateways, switches etc. The IDS uses small amount of resources for data checking and sending the data packets destination node. While creating IDS it must be assumed that no node will be fully trusted. The traditional defense mechanisms must also be used for data transportation. In intrusion detection system we will detect network attacks with the help of sensors that are scattered on the network field. The intrusion detection system stands between the sensor nodes and the base station as shown in Fig. 1. Intrusion detection system has following functionalities:

- It will monitor activities in the network and analyze the problem.
- It will detect all vulnerabilities with the help of audit.
- It also checks abnormal activities in the network.
- It also done operating systems audit.

The intrusion detection systems carries it operation in three different levels. There are three main components in an Intrusion Detection System (IDS) which are as follows:

A. Network Intrusion Detection System (NIDS):

This system performs the analysis for the traffic passing on the whole network. It matches data with the traffic data that have been travelled on the subnets and then adds the information to the library of attacks details. And when attack is detected the system will send the alert message to the administrator.

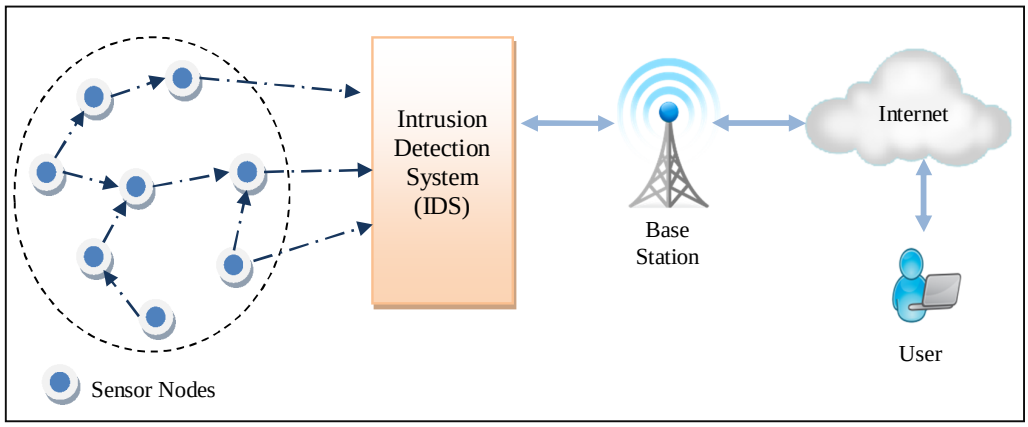


Figure 1. IDS in Wirless Sensor Network

B. Network Node Intrusion Detection System (NNIDS):

It observes network traffic which has passed by network specific node to host. NNIDS monitors only the single host while it cannot monitor the entire network or subnet, and this property differs NNIDS from NIDS.

C. Host Intrusion Detection System (HIDS):

The working of this type of intrusion detection system is by taking snapshots of the current system files and then matching the snapshot with the previous systems files. If in the current snapshot any problem is detected then an alert is generated. The problems such as missing a file may also be alarmed to the administrator.
Wireless sensor networks are always in need of the four major requirements, namely confidentiality, data integrity, service availability and energy. The first three requirements are related to the wireless sensor network's security. The energy is a unique requirement that cannot be fulfilled easily. The four basic needs of WSN are described below:

- Confidentiality: In wireless sensor network data confidentiality is very important when we send data over the network. We must use cryptography mechanisms when we send data in the network. We must encrypt our data before sending using cryptography algorithm. In the network lots of attackers continuously watch our network, if we our data is not confidential means not encrypted then hacker can easily hack our data. In the wireless sensor network data confidentiality is very important to protect our data against attackers.
- Integrity: We used sensor network to monitors environment changes, in wireless sensor network data integrity is very important, because multiple object moving on the field attackers only see physical environment, they retrieve data about where the sensors located. If attacker can retrieve and alter the data then Wireless sensor network will not be able to know what actually attackers have generated. Data integrity is very important to protect our data.
- Availability: Availability is not concern about data being sent in the network, it's related to check network availability for data packet sending, or network functionality not working properly. These problems created because of many issues such as wrong routing information or data packets flooding in the network, etc. Another type of attack is the homing attack, in this attacker finds network traffic and detects critical sensor node and disables this node physically.
- Energy: For attack detection, sensor node requires a lot of battery power. As the battery energy is having limited power it may be difficult to prolong the network's lifetime. For increasing the power for a long time and saving the energy, we send sensor nodes into sleep mode when the nodes remain idle and when

the nodes are required they are again converted into active state. This is one of the methods for saving the battery power of the sensor node.

III Review Of IDS Methods In WSN

In this section, we discuss the different methods presented for the detection of intrusion in WSN. There are different intrusion detection methods based on two basic approaches namely distributed approach and hierarchical approach.

In [1], the author has proposed a protocol that fulfils the unique requirements of WSNs, which is low complexity and energy efficiency. The protocol has two unique properties: firstly it is self-learning and secondly it is distributed in nature. Simple Learning Automata based ID (S-LAID) functions in a distributed manner with each node functioning independently without any knowledge about the adjacent nodes. If a node is compromised it will not affect other working nodes because the network is in distributed format. This schema is based on the concept of stochastic learning automata on packet sampling mechanism, which benefits the proposed work to achieve the goal of energy aware intrusion detection system.

The author has tried to solve the problems of wireless sensor network, by using multi-agent and semantic techniques [2]. Thus, a semantic based intrusion detection framework is proposed. In this IDS security ontology is constructed according to the features of WSN to represent the formal semantics for intrusion detection. The ontology is used to improve the process of intrusion detection. This method uses distributed nature of the network and has a layered architecture of the proposed framework. There are many algorithms proposed by the author and these algorithms have tried to solve the problem in decentralized and cooperative mechanism. In this mechanism, each selected rule of security ontology is mapped to sensing data collected from common sensor nodes to detect anomaly.

The proposed intrusion detection system is a hierarchical design based system for wireless ad-hoc networks. The significant challenge of wireless ad-hoc sensor networks is to maintain the security of the network, and this challenge has been addressed by the author in [3]. The proposed hierarchical design based intrusion detection system fulfils the demands and restrictions of WSN. The intrusion detection system uses policy based detection mechanism. This model follows core defence strategy where cluster-head is the centre point to defend intruder and concentrates on saving the power of sensor nodes by distributing the responsibility of intrusion detection to three layer nodes.

Another IDS method based on hierarchical wireless sensor networks is been proposed in [4]. This method uses routing tables and isolation tables to spot the intrusions and to estimate the usage of IDS. The proposed method isolates malicious nodes by avoiding consumption of unnecessary energy by IDS (ITIDS). The IDS makes use of four different nodes, which are BS, Primary Cluster Head, many Secondary Cluster Heads and the remaining sensor nodes MNs. The ITIDS is based on cluster networks and can detect serious attacks.

As there are inherent disadvantages of static IDS the author proposes a dynamic model of intrusion detection system (DIDS) in [5]. This is a hierarchical model of IDS based on clustered network to battle the low energy problem of sensor networks. It can use distributed defence which has the advantage of detecting multiple intruders, albeit, with an increased rate of energy consumption with increase in cluster size.

A Hybrid Intrusion Detection System (HIDS) has been proposed in cluster based WSN (CWSN) [6]. As the sensor network is cluster based, the nodes in the network may possess different capabilities, and hence, the network is called as heterogeneous wireless sensor network. As the cluster heads and sensor nodes have different capabilities and responsibilities, there should be a hybrid IDS to detect intruders. The cluster head detects the intruders that attempt to decrease the energy consumption as well as reduce the quantity of information in the whole network. Also the proposed IDS proves to be advantageous in prolonging the networks lifetime.

G.V.Crosby et. al., proposed a protocol that detects and isolates the compromised nodes [7]. In addition to reputation based trust framework, the authors have proposed allocation-aware trust-based protocol that not only detects the compromised nodes but also can isolate the node. The wireless sensor network is formed in clusters by using secure cluster formation algorithms. The trust and reputation values are calculated by using a method where the neighbouring nodes monitor each other. A simple location verification algorithm is also proposed. This algorithm has been constructed by utilizing the signal strength information. The simulation results indicated that the protocol effectively detects and isolates the compromised nodes even when the nodes are colluding.

The concept of ontology is used for collecting and organizing the attributes of attacks. But there is a link between ontology concept and lightweight intrusion detection system (IDS). The author explores how the

intrusion detection system about ontology and lightweight IDS are related. Ranger based IDS (RIDS) has been proposed in [8]. It combines the ranger method to reduce energy consumption and the isolation tables to avoid detecting anomaly repeatedly. This lightweight IDS model relates ontology concept mechanism about anomaly detection. In this technique, rough set theory (RST) is used for pre-processing of packets and anomaly models will be trained by support vector machine.

In [9] the author has proposed a detection system, which is deployed on a hierarchical WSN architecture. The author states that, it is difficult to detect a compromised node and to avoid the situation were the victim can be misled by the false information given by the adversary through a compromised node. The proposed scheme is based on the weighted-trust evaluation. The hierarchical architecture of WSN has three types of nodes which makes it a three layered architecture: Access Points (AP) layer, Forwarding Nodes (FN) Layer and the Sensor Nodes (SN) layer. The major assumption made in this scheme is that the base stations are trusted and majority of the sensor nodes are working properly.

Xi Peng et. al., proposed a security management model for self organizing wireless sensor networks based on intrusion detection [10]. It can prevent most of attacks. Then an analysis of each layer of networks in security model is discussed and the security management measures in the data link layer and network layer are described in detail especially. Such a structure is built, based on the existing encryption and authentication protocols.

Byunggil Lee et al., [11] have developed management platform and security framework for WSN. The proposed framework has advantages as regard secure association and intrusion detection. The paper also provides the background of WSN, its security issues and requirements.

Qi Wang et al., [14] have developed an intruder detection algorithm for static wireless sensor networks. The proposed IDS is of low complexity. The intrusion detection model includes characteristics that determine the average frequency of execution of order. A distributed algorithm in which the sensor collects the information from the neighbouring nodes to analyses the anomalies if any from the neighbours. The intrusion detection algorithm on detecting anomalies packets received from its neighbours basic alarms to report the anomaly.

IV. Review Of Homogeneous And Heterogeneous WSN

There are different types of wireless sensor network with different approaches such as single sensing and multi sensing approach. In WSNs with single sensing approach, the network algorithm is not able to detect any type of attack in the wireless sensor network. This type of network is not efficient it will not give guarantee about maximum security against the attacks. And the sensor's battery backup is not good as compare to multi sensing sensors. In wireless sensor networks with multi sensing approach, the algorithm is able detect any type of attack in the sensor network. This network is very efficient; it will give guarantee about maximum protection against attacks. And the multi sensing batteries are rechargeable and having good battery backup as compare to single sensing. There are also wireless sensor networks with different infrastructure such as heterogeneous and homogeneous WSNs. Fig 2. illustrates the heterogeneous and homogeneous WSNs.

A. Homogeneous WSN

In homogeneous network all the nodes are identical in terms of battery energy and hardware complexity. Homogenous networks have pure static clustering. In homogeneous type of network, single network topology is used and this is not a complex network. Thus in short we can say that, sensor network in which the sensor nodes having the similar hardware complexity and battery energy is called as homogenous sensor network. Homogeneous wireless sensor network with pure static clustering is also said to have the possibility where the cluster head nodes should be over loaded with transmissions of long range to remotely situated base stations, also the more processing needed for the protocol coordination and data aggregation [15]. And hence this is resulted into the fact that cluster nodes are expired before the other sensor network nodes. But, one can also ensure that all the sensor nodes expire at the same time, resulting into less residual energy wastage whenever the complete system expires. We can ensure this by rotating role of the cluster head periodically and randomly all the nodes as introduced in the LEACH protocol.

But the most important drawback of homogeneous sensor network as well as role rotation is that all network nodes will be able to act as cluster heads, and hence they should posses the required capabilities related to hardware requirements.

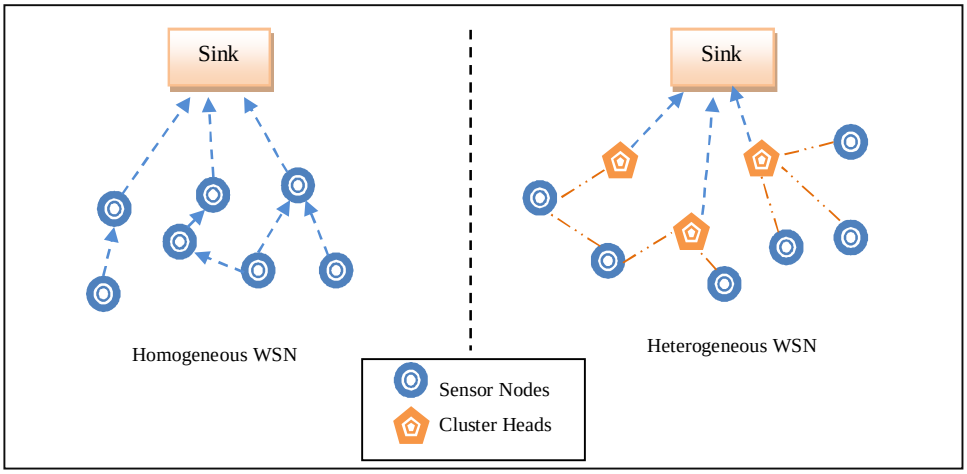


Figure 2. Heterogeneous and Homogeneous WSN

B. Heterogeneous WSN

In heterogeneous networks more than one and different types of nodes with different battery functionality are used. In heterogeneous network different topologies are used and this makes the network a very complex network. Thus in short, we can say that in case of heterogeneous sensor network there are two or more various types of network nodes along with different functionality and battery energy is used. The real motivation behind the heterogeneous networks is the need of extra battery energy and more complex hardware is embedded in some cluster heads, hence this reducing the overall cost of hardware for the remaining sensor network. But the fixing of cluster head nodes is nothing but the role rotation which is not possible longer [13]. Whenever sensor nodes uses the mechanism of single hopping in order to reach cluster head, then sensor nodes those are farthest from cluster head are often spending most of energy as compared to the nodes those are closer to cluster heads. Heterogeneous networks are using the concept of multiple hopping in order to reach the cluster head, the nodes which are closer to cluster head having the more energy burden because of relaying. In addition to this, existence of non uniform energy drainage patter is always there [12, 13]. But the heterogeneous networks adhere with advantage of increasing the lifetime of the wireless sensor network.

Finally, basically there are two kinds of sensor network characteristics such as uniform energy drainage and lower hardware cost. A heterogeneous sensor network achieves lower hardware cost whereas a homogeneous sensor network achieves the uniform energy drainage. However both features cannot be incorporated in the same network.

V. CONCLUSIONS

In this review paper we have reviewed the different intrusion detection methods and systems in WSN, single sensing, multi sensing, homogenous and heterogeneous WSN. As the WSN is consisting of tiny devices called sensors, these devices are having limitations factors such as energy constrained, memory storage, transmission range and computational power. But as per our discussion above, in real time scenarios most of networks are deployed in heterogeneous manner. Therefore, there are two types WSNs such as homogenous and heterogeneous WSN. In this paper we have discussed on two important concepts of wireless sensor networks.

In our proposed work we use heterogeneous type of wireless sensor network with intrusion detection system. As we have surveyed both the concepts, we have implemented the intrusion detection system for detecting packet loss attack and bad mouthing attack. In our future work, we are further plan to use intrusion detection system for detecting more attacks, with energy efficient IDS for heterogeneous WSN. This is because of the several advantages of heterogeneous WSN.

REFERENCES

[1] S. Misra, P. Venkata Krishna and Kiran Isaac Abraham, "Energy Efficient Learning Solution for Intrusion Detection in Wireless Sensor Networks", COMSNETS'10 proceedings of the 2nd international conference on Communication systems and Networks, 2010.

[2] Yuxin Mao, "A Semantic-based Intrusion Detection Framework for Wireless Sensor Network", Networked Computing (INC), 6th International Conference, Gyeongju, Korea, 2010.

[3] M. S. I. Mamun, A.F.M. Sultanul Kabir, "Hierarchical Design Based Intrusion Detection System For Wireless Ad Hoc Sensor Network", International Journal of Network Security & Its Applications (IJNSA), Vol.2, No.3 July 2010.

[4] Rung-Ching Chen, Chia-Fen Hsieh and Yung-Fa Huang, "An Isolation Intrusion Detection System for Hierarchical Wireless Sensor Network", Journal of Networks, Vol. 5, Number 3 March 2010.

[5] G. Huo and Xiaodong Wang, "DIDS: A Dynamic Model of Intrusion Detection System in Wireless Sensor Networks", IEEE, International Conference on Information and Automation, Zhangjiajie, China, June 20 –23, 2008.

[6] K. Q. Yan, S.C. Wang and C.W. Liu, "A Hybrid Intrusion Detection System of Cluster-based Wireless Sensor Networks", Proceedings of the International MultiConference of Engineers and Computer Scientists 2009 , Vol IIMECS 2009 ,Hong Kong, March 18 - 20, 2009.

[7] Garth V. Crosby, Lance Hester, and Niki Pissinou, "Location-aware, Trust-based Detection and Isolation of Compromised Nodes in Wireless Sensor Networks", International Journal of Network Security, Vol.12, No.2, PP.107- 117 March 2011.

[8] Chia-Fen Hsieh, Yung-Fa Huang and Rung-Ching Chen, "A Light-Weight Ranger Intrusion Detection System on Wireless Sensor Networks", published in IEEE Genetic and Evolutionary Computing (ICGEC), 2011.

[9] Idris M. Atakli , Hongbing Hu, Yu Chen, Wei-Shinn Ku, Zhou Su "Malicious Node Detection in Wireless Sensor Networks using Weighted Trust Evaluation", The Symposium on Simulation of Systems Security (SSSS'08), Ottawa, Canada, April 14 –17, 2008.

[10] Xi Peng, Wuhan Zheng Wu, Debao Xiao, Yang Yu,"Study on Security Management Architecture for Sensor Network Based on Intrusion Detection "' IEEE, Volume: 2, 25-26 April 2009.

[11] Byunggil Lee, Seungjo Bae and Dong Won Han, "Design of network management platform and security framework for WSN", IEEE International conference on signal image technology and internet based system, 2008.

[12] B. Liu, P. Brass, O. Dousse, P. Nain, and D. Towsley, "Mobility improves coverage of sensor networks," in Proceedings of the 6th ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc), 2005.

[13] Y. Zhang and W. Lee. Intrusion Detection in Wireless Ad-Hoc Networks. In Proc. ACM MobiCom, pages 275-283, 2000.

[14] Qi Wang, Shu Wang, "Applying an Intrusion detection algorithm to wireless sensor networks", Second international workshop on Knowledge Discovery and Data Mining, 2009.

[15] Y. Wang, X. Wang, B. Xie, D. Wang, and D. P. Agrawal ,"Intrusion detection in homogeneous and heterogeneous wireless sensor networks," IEEE Transactions on Mobile Computing, vol. 7, no. 6, pp. 698–711, 2008.